In The

Supreme Court of the United States

KENNETH F. SODOMSKY,

Petitioner,

vs.

COMMONWEALTH OF PENNSYLVANIA,

Respondent.

On Petition For Writ Of Certiorari To The Supreme Court Of Pennsylvania

PETITION FOR WRIT OF CERTIORARI

DAVID RUDOVSKY, ESQUIRE
Counsel of Record
KAIRYS, RUDOVSKY, MESSING, & FEINBERG, LLP
718 Arch Street, Suite 501S
Philadelphia, PA 19106
(215) 925-4400

PAUL D. BOAS, ESQUIRE
5th Floor, Law and Finance Bldg.
429 Fourth Avenue
Pittsburgh, PA 15219
(412) 391-7707

Counsel for Petitioner

COCKLE LAW BRIEF PRINTING CO (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTION PRESENTED

Where a computer owner leaves his computer for a one-hour upgrade with a computer service provider, and does not authorize access to closed personal files, does the owner either "abandon" his property or forfeit entirely his Fourth Amendment expectation of privacy in the highly personal and private information stored in closed files on the computer's hard drive?

PARTIES TO THE PROCEEDINGS

Petitioner (Petitioner and Appellant below): Kenneth F. Sodomsky

Represented by:

DAVID RUDOVSKY, ESQUIRE
Counsel of Record
KAIRYS, RUDOVSKY, MESSING & FEINBERG, LLP
718 Arch Street, Suite 501S
Philadelphia, PA 19106

PAUL D. BOAS, ESQUIRE
5th Floor, Law and Finance Bldg.
429 Fourth Avenue
Pittsburgh, PA 15219

Respondent (Respondent and Appellee below): Commonwealth of Pennsylvania

Represented by:

ELLEN R. WEST
ASSISTANT DISTRICT ATTORNEY
BUCKS COUNTY DISTRICT ATTORNEY'S OFFICE
633 Court Street
Reading, PA 19601-4317

TABLE OF CONTENTS

	Page
QUESTION PRESENTED	i
PARTIES TO THE PROCEEDINGS	ii
TABLE OF CONTENTS	iii
TABLE OF AUTHORITIES	iv
CITATIONS FOR OPINIONS BELOW	1
BASIS FOR JURISDICTION IN THIS COURT	1
CONSTITUTIONAL AND STATUTORY PROVISIONS AT ISSUE	1
STATEMENT OF CASE	2
CONCLUSION	14

Appendix A: Opinion, Superior Court of Pennsylvania, filed December 5, 2007 ..... App. 1

Appendix B: Order Denying Application of December 19, 2007 ..... App. 19

Appendix C: Opinion, Court of Common Pleas, filed March 6, 2006 ..... App. 20

Appendix D: Order Denying Petition for Allowance of Appeal, Pennsylvania Supreme Court, filed December 16, 2008 ..... App. 39

Appendix E: Letter Extending Filing Date of Petition for Writ of Certiorari ..... App. 40

TABLE OF AUTHORITIES

Page

CASES

Bond v. United States, 529 U.S. 334 (2000) 12

Ferguson v. City of Charleston, 532 U.S. 67 (2001) 8

In re Search of 3817 West End, 321 F.Supp.2d 953 (N.D. Ill. 2004) 7

Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001) 11

O'Connor v. Ortega, 480 U.S. 709 (1981) 11

Rios v. United States, 364 U.S. 253 (1960) 8

Smith v. Maryland, 442 U.S. 735 (1979) 10

Smith v. Ohio, 494 U.S. 541 (1990) 8

United States v. Finley, 477 F.3d 250 (5th Cir. 2007) 12

United States v. Gourde, 440 F.3d 1065 (9th Cir. 2006) 6

United States v. Jacobsen, 466 U.S. 109 (1984) 13

United States v. Mar James, 353 F.3d 606 (8th Cir. 2003) 9

United States v. Miller, 425 U.S. 435 (1976) 10

United States v. Most, 876 F.2d 191 (D.C. Cir. 1989) 8

CITATIONS FOR OPINIONS BELOW

The Order of the Supreme Court (Appendix D) is not reported. The decision of the Superior Court of Pennsylvania (Appendix A) is reported at 939 A.2d 363 (Pa. Super. 2007). The Opinion of the Court of Common Pleas is not reported. (Appendix C).

BASIS FOR JURISDICTION IN THIS COURT

The Supreme Court of Pennsylvania denied review on December 16, 2008. 28 U.S.C. §1254(1) confers jurisdiction on this Court to review on writ of certiorari the Order of the Pennsylvania Supreme Court. On March 10, 2009, Justice Souter granted an application for extension of time to file the Writ of Certiorari to April 14, 2009.

CONSTITUTIONAL AND STATUTORY PROVISIONS AT ISSUE

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT OF THE CASE

1. This is a Petition for Certiorari from the December 16, 2008 Order of the Pennsylvania Supreme Court denying a Petition for Allowance of Appeal from the December 5, 2007 Judgment and Opinion of a panel of the Superior Court reversing the pretrial order of the trial court of Berks County suppressing evidence in a criminal case.

2. On October 15, 2004, Petitioner, Kenneth F. Sodomsky, entered a Circuit City store in Wyomissing, Pennsylvania for the limited purpose of having a DVD drive (player) with burner (hereinafter "DVD drive/burner") installed on his desk top computer. Petitioner delivered to Circuit City his computer (without screen) and the DVD drive/burner that was to be installed. Petitioner informed the clerk that he needed the installation performed quickly, and he was informed that he could return in one hour to pick up his computer. The Circuit City form signed by petitioner authorized Circuit City to undertake a "drive installation," which is explained on the form as "install and configure the optical drive unit and DVD in his desktop computer." App. 2.[1]

Petitioner was not advised by the intake clerk or by the written authorization form that after installation of the new DVD drive, Circuit City employees would access the closed files stored on his hard drive,

---

[1] The facts are taken from the Opinion of the Superior Court of Pennsylvania. Appendix A.

and petitioner neither consented to nor authorized such access. The written authorization form signed by Petitioner stated that the computer was in good working condition.

After the DVD drive and related software were installed without error or problem, another employee, Stephen Richert, arrived at work and proceeded to search the hard drive, looking for a "movie or video." Mr. Richert testified that the reason for his search of petitioner's closed files was to see whether the installation of the DVD drive/burner had distorted them, despite his testimony that the DVD drive/burner software had been successfully installed and that had there been a problem, an indicator of that problem would have appeared on the screen. Mr. Richert testified that he did not test the DVD drive/burner by playing or burning a DVD. Richert acknowledged that the most direct manner for testing the installation, playing a DVD, was not employed. App. 3-5. In fact, the DVD drive/burner was never operated or tested by Circuit City. Mr. Richert testified that he had been asked by a State Police Trooper to alert him to questionable material he might find.

The first several movie files titles accessed by Mr. Richert were "innocuous," and he did not attempt to see whether those files had been "distorted" by the installation. Instead, Richert continued to look at other titles until he came across some with "questionable" names, referring to boys of various ages. Richert opened one such file to view its contents, and not for any reason related to the installation work. Neither

the opening nor viewing of the file involved use of the DVD drive/burner. The witnesses who viewed the video described seeing a penis, and a hand reaching toward, but not touching the penis. There was no specific indication of the age of the male. Circuit City employees then called the Wyomissing police who were shown the same 19 second clip that Richert observed and the police seized the computer without a search warrant. Five days after the computer was seized from Circuit City without a warrant, the police sought and obtained a warrant authorizing the search of the computer. App. 6.

3. On February 15, 2005, a criminal complaint was filed against petitioner. On September 28, 2005 a hearing was held on a Motion to Suppress Evidence filed on behalf of petitioner. The trial court granted the motion to suppress on November 10, 2005. Appendix C.

4. On August 9, 2007, a panel of the Superior Court issued an opinion and order reversing the Order of the trial court. On August 23, 2007, petitioner filed an Application for Reargument En Banc. On September 21, 2007, the panel granted reconsideration and vacated the original August 9, 2007 opinion. Thereafter, on December 5, 2007, the panel issued a new opinion which reversed the decision of the trial court. Appendix A. Petitioner filed an Application for Reargument En Banc, and the Court denied relief on February 7, 2008. A Petition for Allowance of Appeal in the Supreme Court of Pennsylvania was denied on December 16, 2008. App. 39. On March 10, 2009,

Justice Souter granted an extension of time to file this Petition to April 14, 2009.

REASONS FOR ALLOWANCE OF THE WRIT

This Petition presents this Court with the important opportunity to provide much needed guidance on a central issue of today's computer dominated and computer dependent society: Under the Fourth Amendment to the United States Constitution does a computer owner forfeit all rights to privacy *with respect to governmental searches* of the highly personal and private information stored on his computer when the computer is left for a one-hour period of time with a computer service for an upgrade that does not require access of files stored on the hard drive and when the owner of the computer is not informed that any accessing of the closed files will take place?

The Superior Court's opinion is plainly contrary to this Court's search and seizure jurisprudence. That court engaged in a highly flawed analysis of abandonment and privacy doctrine and concluded that whenever a computer owner leaves his or her computer for service, he or she has "abandoned" that property and has lost any expectation of privacy in the personal information stored in the computer, not only with respect to the service repair persons, but to law enforcement officials as well. Computers have become the central repository of personal,

commercial, religious, and private information. For many people the computer is the modern day synthesis of earlier forms of information storage, including diaries, written correspondence, political advocacy, financial accounts, photograph albums, and music collections. The electronic data base of a computer reflects the essential private aspects of the life of the owner. If individual autonomy and privacy are to mean anything in our society, the constitutional preference for warrants must be interpreted in light of these modern developments.

As stated by one federal appellate judge:

> [F]or most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests – including perfect strangers – are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation.

United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J., dissenting)

On a regular basis as well, computer owners need repairs and upgrades to their computers and they regularly rely on commercial enterprises to provide these essential services. The computer networks and links that we all depend upon would quickly break down without these services. In seeking repairs or upgrades, the owner rarely authorizes an invasion of the highly personal information stored in the

computer and most services can be provided without the need to access this information as was the case here. To be sure, there are instances in which access may be necessary, and the owner risks that the service provider (properly or not) will access private information.[2]

The Superior Court sustained the seizure of the computer on two related grounds. First, that petitioner had "abandoned" his property by leaving it for a one-hour service upgrade. Second, that petitioner, by leaving his computer for service at a specific location and under specified written terms, had essentially exposed the contents of the closed files on his hard drive to the entire public, thus forfeiting *any* expectation of privacy vis-à-vis the government in the highly personal and private information stored in secure, closed files within the computer. Based on this supposed forfeiture of all privacy rights, the court determined that the police could seize the computer without a warrant.

Both grounds for decision are fatally flawed. It is absurd to suggest that one "abandons" property by leaving it at a commercial site for a limited repair or

---

[2] The importance of providing a proper standard for seizures and searches of computers is made clear by cases and commentary. *See, e.g.*, Thomas K. Clancy, "The Fourth Amendment Aspects of Computer Searches and Seizures," 75 Miss. L.J. 193 (2005-2006); Orin Kerr, "Searches and Seizures in a Digital World," 119 Harv. L.Rev. 531 (2005); *In re Search of 3817 West End*, 321 F.Supp.2d 953 (N.D. Ill. 2004).

upgrade, with an agreement to retrieve the property within an hour's time. Further, the ruling that all privacy as to the closed files on the hard drive is lost to the entire public, including law enforcement, by the delivery of the computer to the service provider establishes a dangerous precedent.

A. Abandonment

This Court has made clear that one does not "abandon" property unless he plainly relinquished any privacy expectations he had in the property. *See Ferguson v. City of Charleston*, 532 U.S. 67 (2001) (urine sample for medical purposes not abandoned); *Smith v. Ohio*, 494 U.S. 541 (1990) (putting grocery bag on hood of car in response to officer's inquiry is not abandonment); *Rios v. United States*, 364 U.S. 253 (1960) (no abandonment of package dropped to floor of taxi). A person does not abandon his property when he temporarily relinquishes direct control over his belongings. *United States v. Most*, 876 F.2d 191, 196-197 (D.C. Cir. 1989) ("The law . . . does not insist that a person assertively clutch an object in order to retain the protection of the fourth amendment.").

Where an owner of property leaves electronic equipment for a short, designated period of time (here, one hour) with a service center for an upgrade he has not shown any intent to abandon the property. To the contrary, he maintains ownership and ultimate control of the property and has given the service center a limited power (bailment) to make the repair

or upgrade. *See United States v. Mar James*, 353 F.3d 606, 614 (8th Cir. 2003). There is nothing in this typical commercial transaction that reflects any intent to abandon the property. Not surprisingly, the Superior Court of Pennsylvania provided no authority for a finding of abandonment in this type of situation.

Petitioner retained ownership over the computer and its contents, and did not exhibit any clear or unequivocal intent to abandon the closed computer files, or his privacy interests. Petitioner gave no written or verbal authorization for access to the computer's closed files; neither did the installation of the DVD drive/burner require access to the closed files. This Court should reject an "abandonment" doctrine that would defeat all expectations of privacy in private property left for service or repair the moment it is left at commercial premises.

B. Knowing Exposure to the Public

The related and derivative theory relied on by the Superior Court – that petitioner forfeited his expectation of privacy in the computer vis-a-vis the police – when he merely left it for an upgrade, fares no better.[3] The court's decision on this issue poses an

---

[3] While not absolutely clear, it appears that the Superior Court found no reasonable expectation of privacy (and therefore no need for a search warrant) because petitioner had abandoned the computer. The flawed analysis on abandonment also undermines the theory of lost expectation of privacy.

enormous danger to the settled privacy interests of virtually every owner of a computer.

In essence, the court ruled that petitioner should have known that the Circuit City employees would access his closed files, even though such access was not necessary for the installation or testing of the DVD drive/burner, and had not been authorized on the Circuit City form signed by petitioner. The Superior Court held that not only had petitioner lost his expectation of privacy with respect to the employee's viewing of closed files, but that the exposure to a single employee was tantamount to exposure to the entire public, thereby forfeiting all of petitioner's privacy interests in the computer's files.

Some actions taken by individuals so fully disclose what was private that any reasonable expectation of privacy is destroyed. Thus, for example, if one were to disseminate the videos, email messages, or other files on one's computer to the public at large, privacy as to law enforcement would be lost. By the same token, exposure of otherwise private material to a third party may negate a constitutional privacy interest against the government, but only where the information is given to the private party for that party's use. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

Petitioner exhibited a subjective expectation of privacy in the contents of his computer by maintaining those contents in closed files and by restricting Circuit City's access to his computer to that work

stated on the Circuit City authorization form. The Superior Court's ruling that the intake clerk's parting words "[w]e'll make sure it works" apprised petitioner that the closed files on his hard drive would be explored is plainly unjustified. There was no notice that the files on the hard drive would be accessed and viewed; indeed, no access was necessary to perform the upgrade. *See Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (even where an employer had notified the defendant that his computer could be accessed for maintenance purposes or to retrieve a needed document, "there was no evidence that these searches were frequent, widespread, or extensive enough to constitute an atmosphere 'so open to fellow employees or the public that no expectation of privacy is reasonable.'" [*O'Connor v. Ortega*, 480 U.S. 709, 717-718 (1981) (plurality opinion)].

Petitioner did not authorize or consent to a search of the hard drive, request a repair of a problem requiring diagnosis, or request a repair or service that required exploration of his personal files. Because access of the closed files on the hard drive bore no relation to the installation of the DVD drive/ burner, the employee at Circuit City had no legitimate purpose in accessing the files on the hard drive. As such, it was not foreseeable to petitioner that his personal files would be accessed, and petitioner retained an expectation of privacy in the closed files on his hard drive.

Moreover, even if petitioner should somehow have known that his files would be accessed, petitioner did not forfeit his legitimate expectation of privacy, vis-a-vis the government. *See United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (that defendant's employer who owned defendant's cell phone could have read the text messages once defendant returned the phone did not mean that defendant should not have reasonably expected the text messages to be free from intrusion from both the government and the general public.) Exposure to some is not necessarily the equivalent to exposure to all. *See*, *Bond v. United States*, 529 U.S. 334 (2000) (public access to luggage on bus does not permit police to squeeze or manipulate the luggage).

There is an important distinction between the knowing disclosure of otherwise private information to a third party, where one risks disclosure by the third party to the police, and the unregulated access of the police to these materials, which is not permitted absent a showing that the privacy interest has been entirely extinguished by the owner's conduct. In the latter situation one does not forfeit basic privacy interests protected by the Fourth Amendment. In this case, there was no access to the personal files on the hard drive granted by petitioner, and no need for the service provider to access the files. Thus, petitioner preserved his expectation of privacy in these files against invasion by agents of the state.

C. Warrantless Seizure of the Computer

After holding that petitioner had abandoned the computer and, thus, had no expectation of privacy in its contents, the Superior Court held that the warrantless seizure of the computer was permissible under the plain view exception. The Superior Court's ruling in this regard rests entirely on its "abandonment" rationale, and therefore fails if petitioner did not lose all expectations of privacy when he left the computer at Circuit City.

Moreover, the seizure was certain to involve private, personal files on the hard drive. In *United States v. Jacobsen*, 466 U.S. 109 (1984), in allowing the government's temporary seizure of the package following the private search, this Court noted that while the package could no longer support any expectation of privacy, "*it was virtually certain that it contained nothing but contraband.*" *Id.* at 120, n.17 (emphasis added). That concern is even more critical in the instant case, where there was a permanent seizure of the computer containing personal non-contraband information. The police knew that petitioner owned the computer, and that it had been briefly entrusted to Circuit City.

CONCLUSION

The Petition for Writ of Certiorari should be granted.

Respectfully submitted,

DAVID RUDOVSKY, ESQUIRE
Counsel of Record
KAIRYS, RUDOVSKY, MESSING
& FEINBERG, LLP
718 Arch Street, Suite 501S
Philadelphia, PA 19106
(215) 925-4400

PAUL D. BOAS, ESQUIRE
5th Floor, Law and Finance Bldg.
429 Fourth Avenue
Pittsburgh, PA 15219
(412) 391-7707

Counsel for Petitioner

APPENDIX A

2007 PA Super 369

COMMONWEALTH OF PENNSYLVANIA, Appellant	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
KENNETH F. SODOMSKY, Appellee	:	No. 1953 MDA 2005

Appeal from the Order Entered November 9, 2005, in the Court of Common Pleas of Berks County, Criminal Division, at No. CP-06-CR-1025-2005

BEFORE: BENDER, BOWES AND COLVILLE*, JJ.

OPINION BY BOWES, J.: FILED: December 5, 2007

¶ 1 The Commonwealth appeals from the trial court's November 9, 2005 order suppressing evidence.[1] After careful review, we reverse.

> When reviewing a suppression order we follow a clearly defined standard of review and consider only the evidence from the defendant's witnesses together with the evidence from the prosecution that, when read in the context of the entire record, remains

---

* Retired Senior Judge Assigned to the Superior Court.

[1] In its notice of appeal, the Commonwealth certified that the order substantially handicaps its prosecution of this matter; we therefore have jurisdiction pursuant to Pa.R.A.P. 311(d).

> uncontradicted. We are bound by the trial court's findings of fact if those findings are supported by the record, but are not bound by its conclusions of law. *Commonwealth v. Chernosky,* 874 A.2d 123 (Pa.Super. 2005).

Commonwealth v. Steward, 918 A.2d 758, 759 n.1 (Pa.Super. 2007).

¶ 2 The evidence of this matter reveals the following pertinent facts. Richard Kasting was the senior sales assistant in the technology department of the Circuit City Store located on Woodland Road, Wyomissing, Berks County. Mr. Kasting testified that on October 15, 2004, Appellee, Kenneth Sodomsky, came to Circuit City and asked Mr. Kasting to install an optical drive and DVD burner into his computer. The work order that Appellee executed that day authorized Circuit City to install and configure the optical drive unit and DVD in his desktop computer.

¶ 3 In accordance with store practice, Mr. Kasting summarized to Appellee "what is done during the installation." N.T. Suppression Hearing, 9/28/05, at 16. Appellee was informed that as part of the installation process, the installer would "have to make sure [the DVD burner] works." *Id.* at 17. There is no indication that Appellee asked how the DVD burner would be tested or in any manner restricted what procedure could be utilized to confirm the burner's operability. Appellee requested that the work be performed on an expedited basis, and Mr. Kasting instructed him to return in approximately one hour.

¶ 4 Toby Werner was in the middle of the installation process when Stephen Richert, the head of personal computer repairs at that Circuit City, arrived. Mr. Richert testified that the DVD drive was installed when he arrived in the department, but the software had not yet been installed. Mr. Richert explained that all DVD burners and players were accompanied by software.[2] Mr. Richert testified specifically that at Circuit City, with "every installation" of the hardware, "any supplementary software" was installed both as a courtesy "and to make sure when it leaves the store, we can guarantee that it is working." *Id.* at 21.

¶ 5 After the software was installed, Mr. Richert performed a general search for a video to test the new DVD drive. More specifically, he testified as follows:

> Well, after we installed the software, we did a generic search of the PC where you click on the start menu, you click on search, and this being the windows XP, a search box comes up and it is custom made to this operating system. In this case, this system, it's about half way down the screen on the left-hand side there's a search, and you can enter – in this case, you could enter a specific

---

[2] Appellee maintains that he did not request installation of the DVD software. Appellee's brief at 3. However, it is clear that Circuit City could not test the hardware without installing the software and always installed any software accompanying a hardware installation. Appellee was told that the hardware would be tested.

name of a file that you're looking for and find it.

We weren't looking for anything specific, so we did a generic search. Below the field where you could enter the name of a file that you are looking for, you can click on the generic boxes listed, picture, movie or if you click it, it does a general search of the whole PC and finds any of that type of objects that you're looking for. In this case, we clicked movies or video, and it brings up all the different formats of videos.

There are many different types of video formats. There's M-peg, MPG-4, AVI, Quick Time. Any types of those files, if used to place on Windows Media Player, which is a program that's inherent to PC when running windows XP or to the DVD software, in certain circumstances, if you install the software and it wasn't installed properly or you didn't receive notification and you try to play the files or play a DVD movie on the PC, you get distortion that isn't necessarily seen right away when you install it.

So, in this case, we wanted to make sure that all types of files were working fine so that you wouldn't get any type of errors. When you install the different type of software, there's something called code X. It's a little piece of software inside the PC that helps the PC better understand and translate video signals through different players.

> So, in this case, if we play a movie file and we get distorted colors or blurring of the image or a ghosting effect where all color is inverted, we know there is a problem with the installation and we have to find it and fix it. If there is a software update, we have to uninstall and reinstall it, if there was an issue.

Id. at 22-23.

¶ 6 Mr. Richert testified that once the search button was activated for a given object, the computer automatically loaded the requested files onto the screen, which continued to enlarge by itself. Thus, after the search was initiated, Mr. Richert did not manipulate the computer further to see the entire list of videos *Id.* at 30-31. The first few video titles that appeared from Appellee's video list were innocuous. However, as the video log continued to compile on the computer screen, which occurred without any human intervention, some of the files appeared to be pornographic in nature due to their titles which included masculine first names, ages of either thirteen or fourteen, and sexual acts. Mr. Richert clicked on "the first one" that appeared questionable, and the video contained the lower torso of an unclothed male, and when a hand approached the male's penis, Mr. Richert immediately stopped the video. *Id.* at 24. Mr. Richert contacted his manager and then telephoned the Wyomissing police.

¶ 7 During cross-examination, Mr. Richert admitted that he had been told by a Pennsylvania State Police Officer to contact police if he ever ran across what

appeared to be child pornography while at work. At the time, Mr. Richert was taking a course at a local college and hoped to enter the law enforcement field.

¶ 8 Wyomissing Police Detective George Bell and two other police officers responded to the call and viewed the same video clip. When Appellee arrived to retrieve his computer, Detective Bell informed him that his computer was being seized because police suspected that it contained child pornography. Appellee responded that he knew what they had found and that his "life was over." *Id.* at 87. Police took the computer to the police station, obtained a warrant to search it, and discovered child pornography.

¶ 9 On appeal, the Commonwealth maintains that the trial court erred in concluding that Appellee retained a privacy interest in the computer because he volitionally relinquished any expectation of privacy in that item by delivering it to Circuit City employees knowing that those employees were going to install and test a DVD drive. We agree in part with this contention.

¶ 10 We begin our discussion with *Commonwealth v. Shoatz*, 469 Pa. 545, 366 A.2d 1216 (1976), which extensively analyzes whether individuals have the right to contest the search of their personal property after they have abandoned a privacy interest in that item. In *Shoatz*, police were investigating a report that three men were acting suspiciously and appeared to be preparing to burglarize a store. Police initiated surveillance of the threatened premises and

shortly thereafter observed three men, two of whom were carrying suitcases, appear in an alley adjacent to the store. One of the officers approached the men and asked to speak to them. The two men who were carrying suitcases dropped them, and all of the men fled. Police searched the suitcases and discovered illegal weapons. The defendants, who were immediately apprehended, raised constitutional objections to the search of their suitcases. Our Supreme Court concluded that when the defendants dropped their suitcases and ran, they abandoned that property and thus, were not entitled to contest the search.

¶ 11 The Court noted that Pennsylvania has adopted the theory of abandonment, which applies as long as improper police conduct did not induce a defendant's desertion of his personal property. Pursuant to this legal construct, when an individual evidences an intent to relinquish control over personal property, he or she has abandoned a privacy interest in property and cannot object to any ensuing search of the item by police. Abandonment revolves around the issue of intent, which is determined from words, acts, and all relevant circumstances existing at the time the property is purportedly deserted. *Accord Commonwealth v. Sanders,* 595 A.2d 635, 638 (Pa.Super. 1991) ("whether a person reasonably may expect that his or her possessions shall be free from unwarranted governmental intrusion depends on the facts and circumstances").

¶ 12 As the *Shoatz* Court explained, "The issue is not abandonment in the strict property-right sense,

but whether the person prejudiced by the search had voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it at the time of the search." *Shoatz, supra* at 553, 366 A.2d at 1220.

¶ 13 The theory of abandonment is extrapolated from the United States Supreme Court's observation that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States,* 389 U.S. 347, 351-52 (1967) (citations omitted); *see also Oliver v. United States,* 466 U.S. 170 (1984) (defendant did not have reasonable expectation of privacy in his visible real estate containing marijuana).

¶ 14 Our Supreme Court has more recently examined the principle in *Commonwealth v. Hawkins,* 553 Pa. 76, 718 A.2d 265 (1998). In that case, the defendant handed an item to another individual, who then placed it in his mouth. Police seized the individual and extracted the property, which consisted of illicit drugs. Our Supreme Court refused to allow the defendant to object to the seizure of the drugs, noting that under current Fourth Amendment jurisprudence, a defendant cannot object to a search unless he establishes a legitimate expectation of privacy "in the area searched or effects seized" and that such interest

also must be sanctioned by society as reasonable and justifiable. *Id.* at 81, 718 A.2d at 267. It continued that a "legitimate expectation of privacy is absent where an owner or possessor meaningfully abdicates his control, ownership, or possessory interest" in his personal property. *Id.* at 81-82, 718 A.2d at 267. The Court concluded that the defendant had abandoned his expectation of privacy in the drugs by handing them to the drug purchaser and that he had no legitimate expectation of privacy in that individual's mouth. It also refused to grant the defendant derivative standing to object to the search of the drug purchaser's body under the Pennsylvania Constitution.

¶ 15 In the present case, we limit our inquiry to a determination of whether Appellee's expectation of privacy in the videos on the computer that he relinquished to Circuit City employees for repairs was reasonable or whether he knowingly exposed the computer's video files to the public such that he voluntarily abandoned his privacy interest in them. The trial court found that Appellee did retain a privacy interest in the contents of the computer, reasoning that he did not expect the computer's contents "to be published to anyone other than employees of Circuit City as needed to complete the requested installation." Trial Court Opinion, 3/6/06, at 7. In reaching this conclusion, the trial court noted that Appellee did not give Circuit City employees the right to delete files, access financial information, or access his e-mail and so thereby did not lose "all

subjective" expectation of privacy in his computer. *Id.* at 8. Thus, the trial court found the subsequent seizure of the computer to be illegal.

¶ 16 The trial court analogized this case to *Commonwealth v. Davis,* 743 A.2d 946 (Pa.Super. 1999), wherein we held that a tenant did not relinquish his privacy interest in an apartment merely because the landlord had limited access rights to the apartment and that the landlord could not, therefore, consent to a warrantless search of the apartment. Similarly, in *Commonwealth v. DeJohn,* 486 Pa. 32, 403 A.2d 1283 (1979), the Supreme Court found that under the Pennsylvania Constitution, a person retains a privacy interest in bank records, and further held that a bank cannot submit the records to the police in the absence of a search warrant. The *DeJohn* decision was based primarily on the fact that an individual's disclosure of financial records to a bank was not entirely voluntary in that one cannot participate in modern society without obtaining a bank account. The *DeJohn* Court also observed that a customer discloses his financial records to a bank for a limited purpose, to aid in conduct of financial affairs, and that a customer's expectation of privacy is not diminished merely because a bank maintains the records.

¶ 17 Initially, we must observe that the trial court did not employ the proper legal standard. First, the court focused on the irrelevant question of whether Appellee gave Circuit City employees access to financial records and e-mail files. These items were not searched; what Appellee did **not** give employees

permission to do is not the consideration. We must examine whether he did give access or knowingly risk access to his video files, which were the items discovered herein. Furthermore, contrary to the trial court's conclusion, if Appellee exposed the video contents of his computer to Circuit City employees, he abandoned his privacy interest in those computer contents because those employees were members of the public. If Appellee knowingly published his computer video files to members of the public, he had no reasonable expectation, under the applicable law, that the video files would not be disseminated to other individuals, including police.

¶ 18 As noted, abandonment is a question of intent and dependent upon all the attendant facts and circumstances. In accordance with this pertinent standard, we therefore will scrutinize all the facts and circumstances to determine whether Appellee retained a reasonable expectation of privacy in his videos. First, we observe that Appellee gave the employees permission to perform certain actions relative to his computer files. He requested and consented to the installation of a DVD drive and was specifically informed that the drive's operability would be tested by Circuit City employees. Appellee failed to either inquire as to how the DVD drive would be tested or otherwise restrict the employees' access to his computer files for that purpose. Thus, Appellee should have been aware that he faced a risk of exposing the contents of his illegal video files. *Cf. United States v. Barth,* 26 F.Supp. 2d 929 (W.D.Tex.

1998) (computer owner did not lose reasonable expectation of privacy in computer files contained in searched hard drive because owner gave repairman, a confidential informant, hard drive for limited purpose of repairing problem unrelated to files that were searched).

¶ 19 We also find it critical to our analysis that when the child pornography was discovered, the Circuit City employees were testing the DVD drive's operability in a commercially-accepted manner rather than conducting a search for illicit items. *Cf. Barth, id.* Appellee implies that the DVD drive should have been tested by inserting and playing a DVD. Appellee's brief at 3. Nevertheless, as noted, Appellee did not ask how the burner would be tested nor did he place any restrictions regarding the manner of that procedure. As Mr. Richert's testimony indicated, the playing of videos already in the computer was a manner of ensuring that the burner was functioning properly. Once the search for videos was initiated, the list of Appellee's videos appeared automatically on the computer screen. The employee testing the burner was free to select any video for testing purposes, as Appellee had not restricted access to any files. Therefore, Mr. Richert did not engage in a fishing expedition in this case.

¶ 20 The final factor we utilize is the volitional nature of Appellee's actions. In this case, Appellee removed the computer from his home, took the computer to Circuit City, and left it there without either removing the videos containing child pornography or

changing the titles of the videos so that they did not appear to have illegal content. Contrary to the circumstances in *DeJohn, supra,* where a person has little choice but to retain bank accounts in order to function in society, Appellee was not compelled to take this particular computer containing child pornography to the store in the first instance, nor was he forced to leave it there after being informed that the burner's operability would be checked. Appellee was aware of the child pornography and could have elected to leave the store with the computer rather than risk discovery of the pornographic files.

¶ 21 This scenario also stands in contrast with the landlord case relied upon by the trial court. Although landlords routinely retain the right to inspect their premises upon notice, people still retain a privacy expectation in their home despite its status as rental property. Here, however, we find that under the facts and circumstances presented, Appellee knowingly exposed to the public, the Circuit City employees, the contents of his video files. It is clear that Circuit City employees were members of the public; hence, if Appellee knowingly exposed the contents of his video files to them, as members of the public, he no longer retained an expectation of privacy in those videos nor could he expect that they would not be distributed to other people, including police.

¶ 22 As noted, the trial court overlooked the attendant facts and circumstances in this case and improperly focused upon what access rights Appellee had not granted to the Circuit City employees. While the

trial court may or may not be correct that Appellee retained a privacy interest in other computer files, such as e-mail or financial records,[3] he did not retain a privacy interest in his videos under the facts and circumstances herein.

¶ 23 Since Appellee abandoned his privacy interest in the videos contained in the computer, he cannot object to the subsequent viewing of the video list and file by police. As noted, our decision is firmly rooted in current Pennsylvania authority; we therefore reject Appellee's independent reliance on the Pennsylvania Constitution to protest the police actions in this case.

¶ 24 Our result in this case is consistent with the weight of authority in this area. If a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents. *E.g. United States v. Simons,* 206 F.3d 392 (4th Cir. 2000) (where employee was informed that his work-related internet activity would be scrutinized by employer, he had no legitimate expectation of privacy in fruits of his internet activity as he knowingly

---

[3] Since Appellee's e-mail and financial records were not searched, we need not analyze the propriety of the trial court's conclusion that he retained a privacy interest in those files. *But see Commonwealth v. Proetto,* 771 A.2d 823 (Pa.Super. 2001), *aff'd,* 575 Pa. 511, 837 A.2d 1163 (2003) (defendant does not have reasonable expectation of privacy in contents of sent e-mail and chat rooms).

exposed such activity to public); *United States v. King,* 2006 WL 3421253 (M.D.Ala. 2006) (defendant knowingly exposed personal files to public under *Katz* by linking to network after being informed that personal files could and would be searched using network even though defendant attempted to protect files from network search); *Lown v. State,* 172 S.W.3d 753 (Tex.App. 2005) (defendant did not have reasonable expectation of privacy in files on work computer which were backed up at request of people in authority at defendant's company).

¶ 25 As an alternative basis to affirm, Appellee argues that Mr. Richert was acting as an agent of the police when he viewed the pornographic file. However, the theory of abandonment applies specifically to searches conducted by police. Since we find that Appellee abandoned any reasonable expectation of privacy in the contents of the videos, he cannot prevail in his suppression motion regardless of who conducted the search.

¶ 26 Appellee also suggests that the seizure of the computer was improper because it was accomplished without a warrant. We agree with the Commonwealth's assertion that the plain view exception to the warrant requirement applied herein. The plain view doctrine provides that evidence in plain view of the police can be seized without a warrant, *Coolidge v. New Hampshire,* 403 U.S. 443 (1971), as modified by *Horton v. California,* 496 U.S. 128 (1990), and it was adopted by our Supreme Court in *Commonwealth v. McCullum,* 529 Pa. 117, 602 A.2d 313 (1992). The

plain view doctrine applies if 1) police did not violate the Fourth Amendment during the course of their arrival at the location where they viewed the item in question; 2) the item was not obscured and could be seen plainly from that location; 3) the incriminating nature of the item was readily apparent; and 4) police had the lawful right to access the item. *Horton, supra; McCullum, supra; accord Commonwealth v. McCree,* ___ Pa. ___, 924 A.2d 621 (2007).

¶ 27 In the present case, police did not violate the Fourth Amendment in arriving next to the computer. Circuit City, which owned the premises, had granted them permission to enter the repair area though their on-site employees. *Accord McCullum, supra* (where police had permission of tenant to be in apartment, they had lawful vantage point from which to view incriminating evidence); *cf. Commonwealth v. English,* 839 A.2d 1136 (Pa.Super. 2003) (police had plain view of marijuana growing on defendant's porch but violated Fourth Amendment by entering onto premises without warrant, consent, or exigent circumstances; plain view doctrine therefore did not apply). The videos were not obscured in that they could be seen readily from that location.

¶ 28 We also conclude that the incriminating nature of the video files was immediately apparent. Appellee suggests that it was unclear whether the videos depicted child pornography because police could not ascertain the age of the naked male, whose face was not revealed, from the portion of the video that they viewed. We disagree. Appellee ignores the titles

assigned to the videos on his computer. Mr. Richert stated that the titles listed a masculine name, an age of either thirteen years old or fourteen years, and "different types of sexual acts." N.T. Suppression Hearing, 9/28/05, at 24. The video titles, together with the clip of a naked male with a hand reaching for the penis, made it "readily apparent" that the videos were of illegal child pornography. Finally, police had the lawful right to access the videos because, as analyzed extensively above, Appellant had abandoned any reasonable expectation of privacy in them.

¶ 29 Order reversed. Case remanded. Jurisdiction relinquished.

¶ 30 Judge Colville files a Concurring Opinion.

Judgment Entered:

/s/ James D. McCullough
Deputy Prothonotary

Date: December 5, 2007

CONCURRING OPINION BY COLVILLE, J.*:
FILED: December 5, 2007

¶ 1 Appellee's challenge must fail because he did not retain a reasonable expectation of privacy in the videos contained in the computer after delivering it to Circuit City. There being no reasonable expectation of privacy, I would not engage in the Majority's plain view analysis. *See Commonwealth v. Viall,* 890 A.2d 419, 422 (Pa. Super. 2005) (holding that a defendant cannot prevail in a challenge to the search and seizure of evidence if the defendant does not have a legally cognizable expectation of privacy in the property searched).

¶ 2 For these reasons, I concur in the result.

---

* Retired Senior Judge assigned to the Superior Court.

APPENDIX B

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF PENNSYLVANIA
v.	:	
KENNETH F. SODOMSKY	:	No. 1953 MDA 2005

ORDER OF COURT

The Court hereby DENIES the application filed December 19, 2007, requesting reargument or reconsideration of the decision dated December 5, 2007.

PER CURIAM

DATE: February 7, 2008

APPENDIX C

COMMONWEALTH OF PENNSYLVANIA	:	IN THE COURT OF COMMON PLEAS
VS.	:	CRIMINAL DIVISION
KENNETH F. SODOMSKY, Defendant	:	No. CP-06-CR-1025-2005

OPINION,
JEFFREY K. SPRECHER, J. MARCH 6, 2006

A Criminal Information charging the defendant, Kenneth F. Sodomsky, with two counts of Sexual Abuse of Children,[1] and one count of Obscene and Other Sexual Materials and Performances[2] was filed on March 11, 2005 in the Court of Common Pleas of Berks County, Pennsylvania, Criminal Division. On May 23, 2005, the defendant filed an Omnibus Pretrial Motion for Relief requesting suppression of evidence seized during a search of his computer. A hearing on the Motion was held September 28, 2005 and this Court granted the motion for suppression on November 10, 2005. The Commonwealth of Pennsylvania filed a Notice of Appeal from that Order on November 15, 2005.

---

[1] 18 Pa.C.S.A. § 6312(d).

[2] 18 Pa.C.S.A. § 5903(a)(3).

FACTS

On October 15, 2004, the defendant, Kenneth Sodomsky, took a computer to the Circuit City store on Woodland Road in Wyomissing, Berks County, Pennsylvania to have a DVD drive and burner installed into the computer and configured. The items contained software specifically to enable it to run properly. The defendant signed a work order authorizing the work to be done on the computer and asked that it be done quickly. A store employee told the defendant that the work would be finished later that day. He also explained that store employees would make sure the product worked after installation.

After the DVD drive and burner were installed, a store employee ran a generic search for videos on the defendant's computer. He intended to run several types of videos to be sure the items purchased were running properly and to make any necessary adjustments to the ancillary software. The search yielded a list of videos; some with names that the employee suspected may have described child pornography.

The employee selected a file named "12 yo Danny Hottie" for use in testing the DVD player. After watching nineteen seconds of the video, the employee stopped the video, called his manager, and called the Wyomissing Police Department.

This employee had a conversation with Pennsylvania State Trooper Tom McDaniel approximately one month earlier in which they discussed what the

employee should do if he ever found child pornography on a computer. The officer provided his business card to the employee, who was a student of his at the time, and directed him to call if the occasion ever arose. The employee did not have Trooper McDaniel's phone number in his possession when he encountered the video on the defendant's computer.

The selected video portrayed a frontal view of a male approximately from his mid-chest down to his knees. The male was unclothed from just below his waist to just above his knees. A hand then appeared again, moving toward the unclothed male's genitalia. The screen then went blank momentarily.

Officer Phillips of the Wyomissing Police Department arrived and viewed the same portion of the video that the store employee had viewed. Detective George Bell and Detective Yoch of the Wyomissing Police Department arrived at the store and viewed that same portion of the video. Officers waited for the defendant to return to the store. While the computer was being worked on through the time the defendant returned, the computer was in a back room which the public, and most employees were not permitted to enter.

When the defendant returned to the store to retrieve his computer, Detective Bell went out to meet him and asked him to accompany him back to the manager's office. Detective Bell told the defendant that the police were seizing his computer because

there was suspected child pornography on the computer. The defendant replied that he knew what they found; he had not deleted a file that he had received and his "life was over." The computer was taken to the Wyomissing Police Department later that afternoon.

On October 22, 2004, Detective Donald Stewart of the Berks County District Attorney's Office arrived at the Wyomissing Police Department with a search warrant for the computer issued at 5:30 p.m. on October 20, 2004. Detective Steward took the computer to his office, where a forensic search was conducted.

ISSUES

The Commonwealth's Statement of Matters Complained of, filed pursuant to Pennsylvania Rule of Appellate Procedure 1925(b), raises eight issues.

1. Whether this court erred in granting defendant's Motion to Suppress.

2. Whether this court erred in granting the defendant's Motion to Suppress when the defendant lost any subjective expectation of privacy in his computer once he turned it over to Circuit City employees.

3. Whether this court erred in determining that the plain view exception did not apply to the police seizure of the defendant's computer although the trial court determined that the police officers had lawfully

viewed the alleged child pornography on the defendant's computer.

4. Whether this court erred in determining that the plain view exception did not apply to the police seizure of the defendant's computer when the police were lawfully on the premises where the contraband was located and the police had lawfully viewed the alleged child pornography on the defendant's computer.

5. Whether this court erred in determining that the pre-intrusion plain view exception would not support the seizure of the defendant's computer because police did not obtain a warrant before seizing the computer.

6. Whether this court erred in determining that the post-intrusion plain view exception would not support the seizure of the defendant's computer because the police officer's view was not inadvertent pursuant to *Commonwealth* v. *McEnany*, 667 A.2d 1143, 1148 (Pa.Super. 1995).

7. Whether this court erred in failing to determine that, under the facts of this case, the warrantless seizure of the computer was proper because the three conditions for a plain view seizure under *McEnany* were met.

8. Whether this court erred in determining that the warrantless seizure of the defendant's computer was unlawful because no exigent circumstances existed to justify the seizure.

DISCUSSION

General Suppression

Each issue raised in a Concise Statement must be specific in order to permit adequate review. *Commonwealth v McCree*, 857 A.2d 188, 192 (Pa.Super. 2004). The Commonwealth's first stated complaint sets forth the overly broad allegation that this Court erred in granting defendant's Motion to Suppress. Therefore, this allegation will not be directly addressed in this opinion. The Commonwealth's subsequent allegations are more specific statements of this issue and are addressed in the order in which they appear in Commonwealth's Statement of Matters Complained of on Appeal.

Subjective Expectation of Privacy

The Commonwealth alleges that the defendant surrendered any subjective expectation of privacy in his computer once he turned it over to Circuit City. "The Fourth Amendment of the United States Constitution protects people from unreasonable governmental intrusions into their legitimate expectations of privacy." *Commonwealth v. Davis*, 743 A.2d 946, 950 (Pa.Super. 1999) citing *Commonwealth v. Rathfon*, 705 A.2d 448, 450 (Pa.Super.1997), appeal dismissed, 725 A.2d 1209 (Pa. 1999). "While the Pennsylvania Constitution may be employed to guard individual privacy rights against unreasonable searches and seizures more zealously than the federal law, an

individual's expectation of privacy in the place searched must be established to invoke constitutional protection." *Commonwealth v. Viall*, ___ A.2d ___ (Pa.Super. 2005) citing *Commonwealth v. Melilli*, 555 A.2d 1254, 1258 (Pa. 1989). The traditional formulation for standing to contest a search based on an alleged violation of privacy rights under the Pennsylvania Constitution is satisfied when a defendant demonstrates that he has a proprietary or possessory interest in the premises searched. *Commonwealth v. Torres*, 764 A.2d 532, 541-542 (Pa. 2001). Having standing to contest a search based on a proprietary or possessory interest in the premises searched simply entitles the defendant to an adjudication of the merits of his suppression motion; in order to prevail on such a motion, the defendant must also demonstrate that he had a subjective expectation of privacy in the premises at the time of the search and that this expectation was objectively reasonable. *Torres,* 764 A.2d at 542. The determination of whether the person contesting a search and seizure has a legitimate expectation of privacy in the area searched is based upon the totality of the circumstances. *Commonwealth v. Davis,* 743 A.2d 946, 950 (Pa.Super. 1999) citing *Commonwealth v. Ferretti*, 577 A.2d 1375, 1378 (Pa.Super. 1990), *appeal denied*, 589 A.2d 688 (Pa. 1991) (internal citations omitted).

Federal courts have held that the right to privacy attaching to computers,[3] office files,[4] and pagers[5] is similar to the right to privacy in a closed container. Fourth amendment protections extend to closed packages, "wherever they may be." *Ex parte Jackson,* 96 U.S. 727, 733 (1877). In addition,

> The United States Supreme Court has stressed that whether a citizen's enclosed possessions are entitled to Fourth Amendment protection is not dependent on the type of hardware which secures them or the size and sophistication of the container in which they are stored. The Fourth Amendment protects alike the traveler who carries a toothbrush and a few articles of clothing in a paper bag and the sophisticated executive with the locked attaché case.

Commonwealth v. Mason, 637 A.2d 251, 254-255 (Pa. 1993) quoting *Commonwealth v. Brundidge,* 620 A.2d 1115, 1118-1119 (Pa. 1993) (internal quotations omitted). "A container which can support a reasonable expectation of privacy may not be searched, even on probable cause, without a warrant." *California v. Greenwood*, 486 U.S. 35, 46, (1988) quoting *United States v. Jacobsen*, 466 U.S. 109, 120, n. 17 (1984)

---

[3] *United States v. Barth,* 26 F.Supp.2d 929, 936 (W.D. Tex. 1998).

[4] *United States v. Knoll,* 16 F.3d 1313, 1320 (2nd Cir. 1994).

[5] *United States v. Chan*, 830 F.Supp. 531, 534 (N.D.Cal. 1993).

(citations omitted). The contents of the defendant's computer, even when temporarily in the hands of a third party for a limited purpose, can support a reasonable expectation of privacy and may not be searched, even on probable cause, without a warrant.

Here, the defendant granted only very limited rights to his computer to Circuit City. He did not completely suspend his expectation of privacy in the computer. He expected the computer to be returned within a few hours at most. He did not expect it to be damaged or put in the trash. He did not he expect its contents to be deleted or to be published to anyone other than employees of Circuit City as needed to complete the requested installation. He did not grant employees permission to access his personal financial information or emails from his computer. An analogy can be made to *Commonwealth v. Davis*, 743 A.2d 946 (Pa.Super. 1999), where the Superior Court of Pennsylvania held that rights granted to a landlord to perform an announced annual inspection of the tenant's apartment, did not constitute a complete waiver of Fourth Amendment rights by the tenant. *Davis,* 743 A.2d at 951. Regarding a surrendered or shared expectation of privacy, in

> [t]he seminal case of *United States v. Matlock*, the Supreme Court defined the authority of a third party to consent to a search of a dwelling or item. In a footnote, the Supreme Court stated that the authority which justifies the third party consent does not rest upon the law of property . . . but rests rather

> on the mutual use of the property by persons generally having *joint access or control for most purposes*, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

United States v. Barth, 26 F.Supp.2d at 938 quoting *United States v. Matlock,* 415 U.S. 164, 171 n. 7 (1970). The defendant did not grant joint access and control of his computer for most purposes to Circuit City. He granted temporary, restricted access, at an agreed upon time, for an agreed upon function. The defendant did not lose all subjective expectation of privacy in his computer once he contracted with Circuit City to install the DVD drive and burner.

Actions of Private Citizens

"As a general rule, a search and seizure without a warrant is deemed unreasonable for constitutional purposes." *Commonwealth v. Holzer*, 389 A.2d 101, 106 (Pa. 1978). A search relates to privacy rights and a seizure relates to interference with possession. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). There are exceptions to the warrant requirement for searches and seizures by police officers where the warrantless search or seizure "does not amount to a significant invasion of a defendant's reasonable expectations of privacy." *Holzer*, 389 A.2d at 106. "Exceptions falling within this category include

consent, abandoned property, plain view, and actions of private citizens." *Id.* at 106 n. 5.

Here, private citizens who were employees of Circuit City conducted a limited search of the defendant's computer, independent from the police. Police then searched by viewing the same video that the employees had viewed. Police subsequently performed a search beyond the scope of the civilian search by obtaining the serial number from the computer, and then seized the computer. Finally, police conducted a more invasive search one week after the seizure when a search warrant was obtained.

"A search conducted by a private individual is not subject to the restraints of the Fourth Amendment to the United States Constitution." *Commonwealth v. Kozak*, 336 A.2d 387, 389 (Pa. Super. 1975) citing *Burdeau v. McDowell*, 256 U.S. 465 (1921). "Where the search is begun and completed by a private citizen before the police are even aware that a search is being made, and where the police did nothing more than confirm the suspicions of the private citizen, a warrant is not required." *Kozak*, 336 A.2d at 392. In the instant case, "we are not dealing with a case wherein the police requested the search." *Kozak*, 336 A.2d at 389 citing *Corngold v. United States,* 367 F.2d 1 (9th Cir. 1966). "We are instead dealing with a search made entirely by a private citizen on his own initiative with no police participation or control during the search." *Kozak*, 336 A.2d at 389. There is no evidence that the employees were directed to

search computers for pornography in general, nor with respect to this particular computer. Therefore the viewing of the file named "12 yo Danny Hottie" during testing of the newly installed DVD player, was a search by a private individual not subject to the restraints of the Fourth Amendment to the United States Constitution.

"A governmental search infringes a legitimate expectation of privacy only to the extent to which it exceeds the scope of a previous private search." *Commonwealth v. Kean*, 556 A.2d 374, 385 (Pa.Super. 1989). While at the Circuit City Store, police officers only viewed the one file on the defendant's computer which private citizens had viewed. The police officers' viewing of the video file on the defendant's computer at the invitation of private citizens and limited to items viewed by the private citizens, was a reasonable search, not in violation of the defendant's rights of privacy. The defendant had no remaining privacy interest in that file. However, he retained a privacy interest in the remaining contents of the computer and in the computer itself.

In both *Jacobsen* and *Kozak,* it was not important whether the contraband was in plain view when the police arrived or whether the police needed to unwrap a package or open a suitcase to see the contraband. Police were permitted to view the contents of the containers as a consequence of the prior view by a private citizen. "[S]ubsequent warrantless examination of the evidence already found will not render the evidence inadmissible, even if the authorities are

required to reopen the package." *Kozak,* 336 A.2d at 391-392. Viewing the contents of the container was not considered "as an entirely new and separate search, no[r] will we include it as part of [the initial] search." *Kozak,* 336 A.2d at 391. Plain view analysis was not required in these cases, as the applicable exception to the warrant requirement for the search was the prior action of private citizens.

Plain View

In its third through seventh matters complained of on appeal, the Commonwealth alleges that the plain view exception applied to the police seizure of the defendant's computer. Commonwealth's third and fourth allegations are that this exception applies because the police officers had lawfully viewed the alleged child pornography on the computer and were lawfully on the premises where the alleged contraband was located. Commonwealth's fifth allegation is that because the pre-intrusion plain view exception applies, the police did not need a warrant in order to seize the computer. The sixth and seventh matters both allege that the post-intrusion plain-view exception applies and supports the warrantless seizure. These related allegations are addressed jointly.

The plain view exception can apply when police officers are lawfully in a protected area and observe contraband in plain view (post-intrusion plain view). In this case, police lawfully entered a protected area, a private office in the Circuit City store, with the

express consent of store employees. In order to seize an item without a warrant in situations where the plain view occurs after an intrusion into a constitutionally protected area, the following three conditions must be met: "(1) the initial intrusion must be lawful; (2) the item must have been inadvertently observed; and (3) there must be probable cause to link the observed property with criminal activity." *Commonwealth v. McEnany*, 667 A.2d 1143, 1148 (Pa.Super. 1995) citing *Commonwealth v. Daniels*, 593 A.2d 895, 897 (Pa.Super. 1991). Probable cause requires

> that the facts available to the officer would warrant a man of reasonable caution in the belief that certain items may be contraband or stolen property or useful as evidence of a crime; it does not demand any showing that such a belief be correct or more likely true than false. A practical, non-technical probability that incriminating evidence is involved is all that is required.

McEnany, 667 A.2d at 1148 (internal quotations omitted) (emphasis omitted). A review of the video in question indicates that there was probable cause to link the observed property with criminal activity.

The post-intrusion plain view exception does not apply in this case because the view was not inadvertent, and in fact there was no plain view. Police officers entered Circuit City with the express intent of viewing a video suspected of containing child pornography. There was nothing inadvertent about their view. The officers were not in the store, let alone the

private room, for any other purpose than to view this video. There is no evidence of contraband in plain view. After entering the private room, police could observe a closed container, a computer, which did not immediately appear to be incriminating. The computer itself was not contraband. It could be compared to opening a file cabinet or to opening a closed container with multiple compartments, which was previously opened by private citizens. The file had to be opened and played in order to view anything even remotely incriminating. In order to actually observe the item of suspected contraband, police had to request that employees play the video. Viewing the video inside the computer was a second lawful entrance into a protected area. The view was not inadvertent; therefore, the post intrusion plain view exception would not support warrantless seizure of the defendant's computer.

The plain view exception may also apply where police officers are not in a protected area and observe contraband in a protected area. The standard for pre-intrusion plain view is set forth in *Commonwealth v. English*, 839 A.2d 1136, (Pa.Super. 2003). "The second line of cases involves situations where the [plain] view takes place before any intrusion into a constitutionally protected area." *English,* 839 A.2d at 1140. In such cases, it is not required that the view be inadvertent; however, absent another exception, the item cannot be seized without a warrant. *English*, 839 A.2d at 1140. The view in this case was not a pre-intrusion plain view because police entered the

private, constitutionally protected, area of the store and entered the defendant's computer prior to viewing the suspect file. The room was not open to the public; therefore, the storeowner and employees had a legitimate expectation of privacy in that room. Officers were only permitted into that room at the express consent of store employees under the consent exception to the prohibition against a warrantless search. Even after entering the private room, police did not observe contraband in plain view.

There was no pre-intrusion plain-view; therefore, the pre-intrusion plain-view exception does not support seizure of the defendant's computer without a warrant.[6] Even if this were a pre-intrusion case, officers would need a warrant to seize a computer

---

[6] The Pennsylvania Supreme Court has permitted warrantless seizures of items in an automobile when "(1) an officer views the object from a lawful vantage point and (2) it is immediately apparent to him that the object is incriminating." *Commonwealth v. Ballard*, 806 A.2d 889, 891-892 (Pa.Super. 2002) citing *Commonwealth v. Petroll*, 738 A.2d 993, 999 (Pa. 1999) (internal citations omitted). If the facts in this case were such that the computer file was in plain view from an unprotected area, the situation would remain distinguishable from *Ballard*. In Circuit City, the computer is subject to greater protections than in an automobile due to its location in an enclosed room of a private business, not at all visible to the public. In addition, seizing of an entire computer is akin to seizing one's entire file cabinet or automobile rather than the one incriminating item. The typical computer would contain many files and much of one's personal and financial information. A warrant would be required to seize a computer from this location.

observed in plain view. Viewing of the video at the store was a lawful search only because police limited their search to the file that private citizens had viewed.

Exigent Circumstances

The Commonwealth's eighth and final complaint is that exigent circumstances existed to justify seizure of the defendant's computer. The exigent circumstances exception to the warrant requirement exists when "the need for prompt police action is imperative, either because evidence sought to be preserved is likely to be destroyed or secreted from investigation, or because the officer must protect himself from danger to his person by checking for concealed weapons." *Holzer,* 389 A.2d at 106. With regard to exigent circumstances, "there can be no inflexible standard; instead the reasonableness of searches and seizures must necessarily be determined on a case-by-case basis." *Commonwealth v. Williams*, 602 A.2d 350, 354 (Pa.Super.1992).

Upon arrival at Circuit City to retrieve his computer, the defendant was unaware that police officers had viewed his computer. There was no evidence of suspicion on his part that would lead to destruction of the evidence. The defendant could have reclaimed his computer with no knowledge whatsoever of police activity. There is no evidence of danger to the police. The defendant did not make any effort to take the computer or remove the computer from the store.

Pretrial Hrg. Transcr. 73:15-23. Therefore, no exigent circumstances existed. Further, the seizure was not a minor interruption of the defendant's possessory interest. The seizure was a substantial invasion of a protected interest as the police retained the computer for five days without a search warrant.

There was testimony that police were waiting in the store for the defendant to return to the store. Pretrial Hrg. Transcr. 43:14-20. It is clear that while the defendant was in the store, the police advised him that they were taking the computer. Upon viewing the suspected child pornography, the officers could have made immediate application for a search warrant. In the event that the officers did not have the time to complete the application, they could have allowed the defendant to take the computer, followed the defendant to confirm the location of the computer, and then obtained the search warrant. Alternately, they could have advised him that they wanted to seize the computer and were in the process of obtaining a warrant, and then requested his consent. These options were not pursued because a detective with the Berks County District Attorney's office advised the police officers that no search warrant was required to seize the computer.

"Under the Supreme Court's current Fourth Amendment jurisprudence, government conduct may violate the Fourth Amendment if it unreasonably invades one's reasonable expectations of privacy or one's ownership or possessory interests in certain property." *U.S. v. Conley,* 856 F.Supp. 1010, 1019

(W.D.Pa. 1994). Seizure of the defendant's computer without a warrant was an unreasonable seizure. The exclusionary rule requires suppression of any evidence found unless the government can demonstrate that a significant break in the causal chain occurred "between the illegality and the seizure of evidence." *Commonwealth v. Ayala*, 791 A.2d 1202, 1209 (Pa.Super. 2002) quoting *Commonwealth v. Strickler*, 757 A.2d 884, 889 (Pa. 2000). All items that officers located in the Defendant's computer after removing it from Circuit City were viewed as a direct result of the unlawful seizure; therefore, these items will be suppressed as a fruit of the poisonous tree. *Ayala*, 791 A.2d at 1211 citing *Commonwealth v. Freeman*, 757 A.2d 903, 906 (Pa. 2000). For these reasons, the Court respectfully requests that the Commonwealth's appeal be denied and the evidence suppressed.

BY THE COURT:

/s/ JKS
JEFFREY K. SPRECHER, J.

APPENDIX D

IN THE SUPREME COURT OF PENNSYLVANIA MIDDLE DISTRICT

COMMONWEALTH OF PENNSYLVANIA,	:	No. 140 MAL 2008
Respondent	:	Petition for Allowance of Appeal from the Order of the Superior Court
v.	:	
KENNETH F. SODOMSKY,	:	
Petitioner	:	

ORDER

PER CURIAM:

AND NOW, this 16th day of December, 2008, the Petition for Allowance of Appeal is hereby DENIED.

APPENDIX E

Supreme Court of the United States
Office of the Clerk
Washington, DC 20543-0001

William K. Suter
Clerk of the Court
(202) 479-3011

March 10, 2009

Mr. Paul D. Boas
5th Floor, Law & Finance Building
429 Fourth Avenue
Pittsburgh, PA 15219

Re: Kenneth F. Sodomsky
v. Pennsylvania
Application No. 08A787

Dear Mr. Boas:

The application for an extension of time within which to file a petition for a writ of certiorari in the above-entitled case has been presented to Justice Souter, who on March 10, 2009 extended the time to and including April 14, 2009.

This letter has been sent to those designated on the attached notification list.

Sincerely,

William K. Suter, Clerk

by

Sandy Spagnolo
Case Analyst